Proceedings of the 5th International conference on e-learning 2010, Penang, Malaysia, 12-13 July 2010, Pages 282-290, ISBN 978-1-906638-69-6

Information Security in eLearning: A Discussion of Empirical Data on Information Security and eLearning

Najwa Hayaati Mohd Alwi and Ip-Shing Fan
Cranfield University, UK
n.h.mohdalwi@cranfield.ac.uk
i.s.fan@cranfield.ac.uk

Abstract*:* ELearning systems are increasingly used by educational institutions to support their academic activities. A simple use of an eLearning system is to make materials and notes available to students at anytime and anywhere; more sophisticated uses of eLearning support the interaction and assessment processes. Depending on how eLearning systems are used, information security issues such as intellectual property protection, personal data protection and continuity of service can become significant for educational institutions. However, use of the Internet also creates exposure to information security threats, which may be classified into interruption, interception, fabrication and modification. This paper presents a study of the benefits, growth, implementation and challenges of eLearning today. An online survey was conducted to review eLearning practitioners' perceptions of information security threats; respondents were invited to participate in the survey via e-mail to the 20 *Joint Information Systems Committee* (JISC) mailing list groups related to eLearning in the UK. Using empirical data collected from eLearning practitioners, the relationship between the eLearning entity (users, institution categories, level of information security awareness) and information security threats is discussed. This paper also discusses the perception of information security incidents occurring in eLearning and the impact of information security threats on the different types of users, as well as approaches to information security management. This paper concludes with the suggestion that information security management should be implemented in the preparation of a secured eLearning environment, and draws significant insight from the existing status of information security in eLearning that could be useful for eLearning providers and practitioners.

Keywords: eLearning, challenges, information security management, threats

1. Introduction

Security in eLearning needs to be addressed as a result of exposure to information security threats on the Internet. Although the Internet is a valuable resource for information and knowledge, it has also become the means for a new set of illegal activities. Information on the Internet is always exposed to security threats; so as a consequence of eLearning's dependence on the Internet, the eLearning environment is also affected by information security threats. Many institutions are rushing into adopting eLearning without carefully planning for and understanding the security concerns. Issues such as legitimate users, course content reliability and accessibility (which include admissibility and availability) and others need to be carefully addressed in order to ensure the learning process can effectively take place. This paper will discuss the benefits, growth, implementation and challenges of eLearning today, and will then proceed with a discussion of empirical data regarding the relationship between eLearning and information security threats.

2. ELearning benefit and growth

ELearning offers everyone the chance to be a learner. The concept of anytime, anywhere, learning promotes lifelong learning and makes distance a problem of the past. The flexibility that eLearning offers to students is the main motivating factor behind choosing online courses (Jain and Ngoh, 2003). According to Khan (Khan, 2004), eLearning provides opportunities to create well-designed, learner-centred, engaging, interactive, affordable, efficient, easily accessible, flexible and meaningful distributed and facilitated eLearning environments. Students can save money and time otherwise spent on travelling and obtaining study materials, and can reduce printing costs by reading the available learning material online. ELearning also allows students wider access to limited resources such as eJournals and eBooks, and can support students in enhancing their learning. Improved communication links and better student access encourage them to participate more; they can engage in a public forum with their peers or communicate privately with the lecturer or instructor. Another benefit offered by eLearning is faster delivery of assessments (Chin, 2004); lecturers can give feedback faster compared with traditional methods and peer group students can also provide feedback amongst themselves.

Regardless of the claim that many eLearning initiatives have fallen short of expectation, the market for eLearning is growing (Hamid, 2002). Reports from the Sloan Foundation indicate that 3.5 million students (representing nearly 20% of all U.S higher education students) enrolled in at least one online

course during the Fall 2007 term (Allen and Seaman, 2007). This growth is fuelled by new institutions entering the online arena combined with continuous student demand for online learning options. The need for knowledge among workers has also contributed to the growth of eLearning. All employees need to equip themselves with the necessary knowledge and skills; the easiest way to do this is to enroll themselves as eLearning students.

The functionality of eLearning has also grown in parallel with the need for and development of technology. Figure 1 shows the growth in eLearning functionality. The first step in eLearning was putting the learning content on the Internet so it was accessible by the user at anytime and anywhere (asynchronous learning). Then it broadened to allow the learning session to be conducted on an anytime and anywhere basis (synchronous learning) for all users (instructor/lecturer and students). ELearning now permits registration, assessment and the posting of graduation certificates online. With the intention of adding more flexibility, mobile learning has been introduced. As the functionality of eLearning keeps on growing, the eLearning environment needs to be secured; the increased functionality presented to users makes the eLearning environment more open and exposes it to all kinds of situation including information security threats.

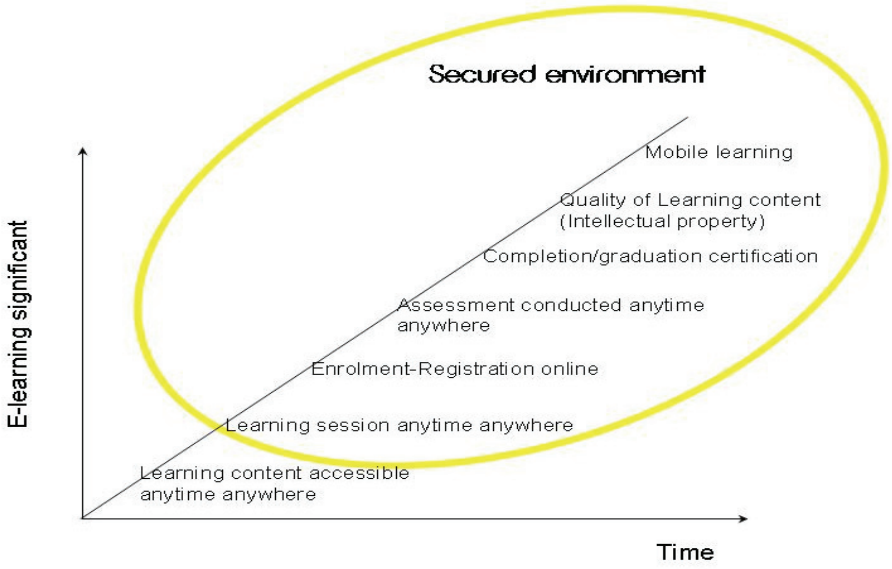

Figure 1: ELearning functionality growth (source: (Alwi and Fan, 2009)

3. Implementation and challenges in eLearning

Implementing eLearning is not an easy task. Despite the many benefits of eLearning, there are challenges in making eLearning implementation successful, which come from two perspectives: the learning provider and the user. Figure 2 reflects the eLearning challenges. The learning provider has challenges in preparing an efficient infrastructure, quality learning material and handling the high cost of implementation. As a result of the widening of eLearning functionality and increased use of the Internet, information security in eLearning can be considered to be a new challenge.

Information security in eLearning has rarely been discussed; it has been ignored (El-Khatib et al., 2003) and neglected (Raitman et al., 2005). Information security is the protection of information from threats; in the context of eLearning, it is implemented to ensure business continuity and minimise business risk, while at the same time maximising return on investment and business opportunities.

In eLearning, information is the organisation's main asset; users, whether staff or student, rely on the information on the eLearning system for their needs. Ensuring the availability and integrity of information is therefore the main goal in eLearning security. While the functionality of eLearning is expanding, the information must be protected in the broader context to avoid any loss of its confidentiality, integrity and availability (Lim and Jin, 2006). At the moment there is no explicit model or framework for information security in eLearning, even though there are standards and models for eLearning and for securing an organisation. In order to define further steps to counter this new challenge, studies need to be conducted. The first aspect is to examine users' perceptions of security in eLearning and consider if users from different groups reflect different perceptions.

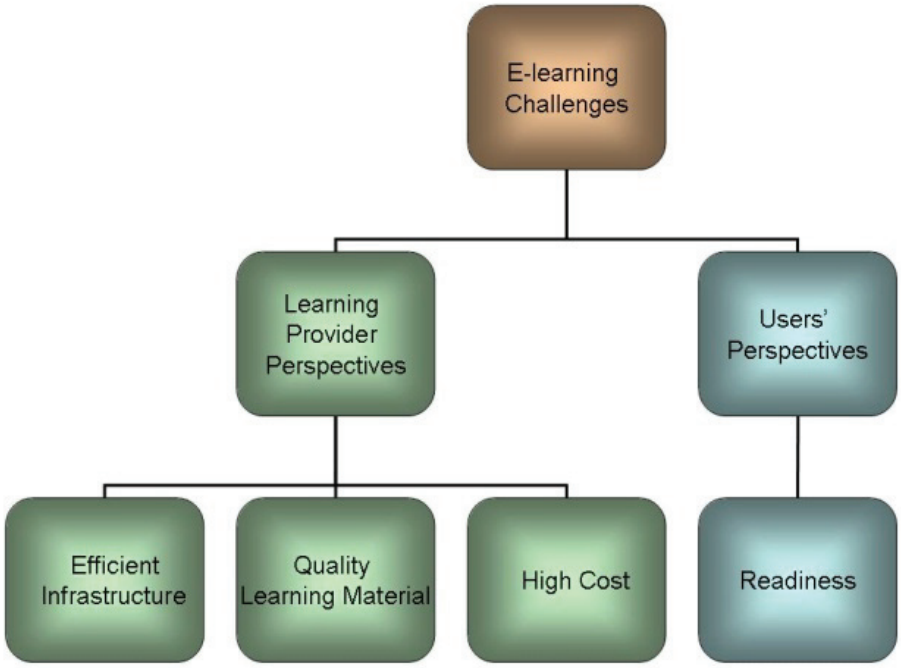

Figure 2: ELearning challenges (source: (Alwi and Fan, 2009)

4. Theoretical framework

In ensuring a functional eLearning environment, the content and services to the users must be interoperable, usable, manageable and durable (Norman and Da Costa, 2003). A functional eLearning includes the users' security and users' protection. At present, information security technology hardware and software are being used to secure eLearning environments either as the preventive or detective control. In order to secure the eLearning environment, it is important to understand the perception of users towards the security threats and issues in eLearning environment. This will help in identifying what is needed to be protected and how best to protect it (Adams and Blandford, 2003). Users in an eLearning environment consist of two main groups which are the supply and the demand group. The supply group are the people who ensure the teaching and learning take place in eLearning environment. This group may consist of people from management, education and technical background. The demand group are the client of the eLearning services which are the students. This study only focused on the supply group by looking at their perception on information security threats in eLearning. The objectives of this study are to confirm whether the user's role has influenced in the perception on information security threats, the user's institution has influenced in the perception on information security threats and the level of information security awareness has influenced the users' perceptions on security. In this study, the influence will be analysed as a relationship between the eLearning entity (users, institution categories, level of information security awareness) and information security threats.

5. Empirical data on information security in eLearning

An online survey was conducted in order to understand users' perceptions of information security threats in an eLearning environment. The targeted respondents were practitioners of eLearning, such as instructors and IT support and administrative staff, from higher learning institutions, further education institutions and training institutions using eLearning. The online survey was protected by secure socket layer level three. It was open for responses for two months from 30th November 2008 to 31st January 2009. Respondents were invited to participate in the survey from mailing list groups in the UK. In order to determine if they were qualified or experienced enough to answer subsequent questions, a filter or contingency question was asked. The questionnaire was developed based on the literature reviews and consisted of 24 questions with multiple sub-questions, divided into 3 sections: user background; institution background; and information security threats. Most of the questions were structured on a five-point Likert scale.

Invitations to participate in this survey were issued to the 20 Joint Information Systems Committee (JISC) mailing list groups related to eLearning. The JISC is the committee funded by the United Kingdom Higher Education and Further Education funding bodies to provide world-class leadership in the innovative use of ICT to support education and research. Even though the invitations were issued to the 20 mailing list groups, some members of the groups were redundant. 115 respondents started the survey; however, only 50 completed it. Many of them decided not to continue answering the questions because they said they didn't know the answers. After considering the filter or contingency question, 48 completed surveys could be used, giving an effective response rate of 41.7%. Table 1 summarises the users' profiles and provides descriptive statistics on the respondents.

Table 1: Summary of the users' profile and descriptive statistics on the respondents

Subject Demographic (n=48)		
Measure and items	Response Frequency (%)	Response Count
Computer Literacy		
Low	0.0	0
Medium	18.8	9
High	81.2	39*
Security Awareness		
Low	0.0	0
Medium	45.8	22
High	54.2	26*
Working experience in eLearning environment (years)		
Less than 1	12.5	6
Between 1- 5	41.7	20*
Between 6-10	29.2	14
More than 10	16.7	8
Number of years institution has been operating an eLearning environment		
Less than 1 year	2.1	1
Between 1- 5 years	35.4	17
Between 6-10 years	50.0	24*
More than 10 years	12.5	6
*mode= the most frequent		

The data were analysed using cross-tabulation (crosstab) to find the relationship between the users' roles and their perception of security, the relationship between the type of institution and perceptions of security and the relationship of security awareness level among users and their perception of security. A rating average was calculated to identify the respondent's tendency towards choice of answer; the rating average is the weighted average per column and row. Table 2 shows the result of the crosstab analysis of questions on security in eLearning and user roles, type of institution and level of awareness. Here the first rating scale choice was valued at 1 (Strongly Disagree), the second at 2 (Disagree), the third at 3 (Neutral), the fourth at 4 (Agree) and the fifth at 5 (Strongly Agree). A response rating of, for example, 3.60 meant that the response fell to the right of neutral and closer to the agree rating. Respondents were asked to state their agreement with the following statements:

- Q1: The eLearning environment is prone to information security threats.
- Q2: My eLearning institution is highly secured.
- Q3: My eLearning institution has information that is highly confidential.
- Q4: My eLearning institution would face significant business disruption if the information were corrupted.
- Q5: My eLearning institution would face significant business disruption if the information were not available.
- Q6: My eLearning institution spends a lot on security controls.
- Q7: My eLearning institution spends a lot on security solutions and recovery.

Table 2: Crosstab on perception of information security threats in eLearning based on users' roles, type of institution and level of awareness

	Role				Type of Institution			Level of Awareness	
	Manage-ment	Educator	IT	Others	Higher Education	Further Education	Training	Higher	Medium
Q1	3.80	3.00	4.67	3.11	3.17	3.75	3.60	3.27	3.35
Q2	3.90	3.82	4.33	3.67	3.77	4.00	3.80	3.50	4.08
Q3	4.30	3.24	4.67	3.50	3.63	3.38	4.20	3.41	3.85
Q4	4.00	4.00	3.67	3.67	3.86	3.75	4.00	3.73	3.96
Q5	4.20	4.06	3.67	3.78	4.06	3.38	4.20	3.91	4.00
Q6	3.40	3.47	4.00	3.61	3.54	3.38	3.80	3.32	3.73
Q7	3.60	3.29	4.33	3.44	3.49	3.13	4.00	3.32	3.62

The data showed that all responses ranged from Neutral towards Strongly Agree with regards to security in eLearning. This demonstrating the respondents agreed that eLearning is prone to threats even though they perceived that their own eLearning institution was highly secured. Similar opinions were held in regard to the subsequent questions. The data also reflects that there were no significant different on perceptions of security depending on each user's role, type of institution and level of security awareness.

In Table 3, the results were crosstabbed to look at respondents from different users' role groups- management, educator, IT personnel and other. Each group was divided to reflect differing levels of security awareness- high, medium and low. None of the respondent claimed that they have low level awareness therefore the table only shows two level awareness – high and medium. Data showed that all responses ranged from Neutral towards Strongly Agree, however the level of awareness does not reflects any significant relation with their perception towards the security questions. People with high level of awareness should have higher awareness that eLearning is prone to information security threats but not all group of the average rating data in the table 3 reflect that.

Table 3: Crosstab of user types with different levels of awareness of perceptions of information security in eLearning

	Role within the institution							
	Management (10)		**Educator (17)**		**IT Personnel (3)**		**Other (18)**	
Awareness	**Higher (5)**	**Medium (5)**	**Higher (10)**	**Medium (7)**	**Higher (2)**	**Medium (1)**	**Higher (9)**	**Medium (9)**
Q1: ELearning environment is prone to information security threats								
	4.40	3.20	2.70	3.43	4.50	5.00	3.22	3.00
Q2: My eLearning institution is highly secured								
	4.00	3.80	3.90	3.71	5.00	3.00	4.11	3.22
Q3: My eLearning institution has information that is highly confidential								
	4.40	4.20	3.50	2.86	4.50	5.00	3.78	3.22
Q4: My eLearning institution would face significant business disruption if the information was corrupted								
	4.00	4.00	4.20	3.71	3.50	4.00	3.78	3.56
Q5: My eLearning institution would face significant business disruption if the information was not available								
	4.00	4.40	4.20	3.86	3.50	4.00	3.89	3.67
Q6: My eLearning institution spends a lot on security controls								
	3.40	3.40	3.60	3.29	4.50	3.00	3.89	3.33
Q7: My eLearning institution spends a lot on security solutions and recovery								
	3.40	3.80	3.50	3.00	4.50	4.00	3.67	3.22

Table 4 shows the crosstab results of user types with different levels of awareness level with regards to their concerns about issues and challenges in eLearning institutions. Here, the first rating scale choice was valued at 1 (Not a Concern), the second at 2 (Minimal Concern), the third at 3 (Some Concern), the fourth at 4 (Concern) and the fifth at 5 (Extremely Concerned). The data showed that

the user are concern about the issues and challenges in eLearning institution and their level of concern are ranging from minimal to extremely concern. However the higher level of awareness does not necessarily shows that they are more concern than the medium level of awareness. Therefore the level of awareness does not show significant relation with the level of concern.

Table 4: Crosstab of user types with different awareness level on issues and challenges in eLearning institutions

	Role within the institution							
	Management (10)		**Educator (17)**		**IT Personnel (3)**		**Other (18)**	
Awareness	**Higher (5)**	**Medium (5)**	**Higher (10)**	**Medium (7)**	**Higher (2)**	**Medium (1)**	**Higher (9)**	**Medium (9)**
Malicious code infection (viruses, Trojan horse, worms)								
	3.60	3.20	3.60	3.43	4.50	4.00	3.22	3.11
Loss of privacy / confidentiality (abuse or misuse of data)								
	3.80	4.20	4.20	3.29	5.00	5.00	3.67	3.89
Electronic exploits/tools (cracking, eavesdropping, spoofing)								
	3.40	3.20	3.30	3.00	4.50	5.00	3.22	3.44
System unavailability (Denial of Service (DOS), natural disasters, power interruptions, bugs)								
	3.40	4.00	4.10	3.71	5.00	3.00	3.22	3.67
Employee misconduct involving information systems								
	2.80	2.00	3.40	2.71	4.50	2.00	2.67	3.11
Spam								
	2.40	2.60	4.00	2.57	4.00	2.00	3.22	3.67
Misconduct involving third parties with access to information systems								
	2.60	2.80	3.30	3.00	4.50	2.00	2.78	3.33
Theft of proprietary information								
	2.60	2.40	3.50	2.43	5.00	3.00	3.11	3.44

Table 5 shows the crosstab of users' perceptions of the most disruptive incidents within the eLearning environment. Here the first rating scale choice was valued at 1 (Unknown), the second at 2 (Insignificant), the third at 3 (Very Minor), the fourth at 4 (Minor) and the fifth at 5 (Major) and the sixth (Very Major). All of the answers were in the range Unknown to Very Minor; this could be because respondents were unaware of such incident or because the information had been kept confidential.

User responses on their perceptions of financial losses caused by security incidents in the eLearning environment is shown in Table 6. Most respondents chose Unknown, as per the rating scale, whether they were of higher awareness or medium awareness.

6. Discussion

ELearning features different groups of users based on their roles. These different groups may have different perceptions on information security issues and on the impact of security incidents. However, the survey conducted has showed that there is no significant relationship between the eLearning entity (users, institution categories, and level of information security awareness) and information security threats; the data has reflected that all users have similar perceptions of security within eLearning. Whatever roles that they are playing, most of the users agreed that eLearning are expose to the information security threats.

The perception of information security incidents occurring in eLearning and the impact of information security threats were no different by types of users; the survey revealed that the users' perceptions of security in eLearning had small and insignificant differences for each type of user. Some of the data received demonstrate that the respondents did not have or were not aware of some particular information. As an example, when users were asked about the impact of incidents, many responded Unknown; this could be as a result of confidentiality about information security in their institutions. The empirical data collected from the survey was enlightening in that clearly users are not fully aware of

the information security situation within eLearning. Therefore it would be beneficial to make users aware of any incidents which have happened or might happen, and any impact of such an incident, in order to increase the security conscious. Having aware of those, make the users consider the controls that can be implemented to secure the eLearning.

Table 5: Crosstab of users' perceptions of the most disruptive incidents within the eLearning environment

	Role within the institution							
	Management (10)		**Educator (17)**		**IT Personnel (3)**		**Other (18)**	
Awareness	**High (5)**	**Medium (5)**	**High (10)**	**Medium (7)**	**High (2)**	**Medium (1)**	**High (9)**	**Medium (9)**
Installation / use of unauthorised software								
	2.20	1.60	2.20	2.43	2.50	2.00	2.22	2.00
Use of institution computing resources for illegal or illicit communications or activities (porn surfing, e-mail harassment)								
	1.80	2.00	2.00	2.86	2.50	2.00	2.56	1.67
Abuse of computer access controls								
	2.00	1.80	1.90	2.14	2.50	2.00	2.22	2.56
Unauthorised access by outsiders								
	1.60	1.20	2.30	1.57	2.50	4.00	1.67	2.11
Physical theft, sabotage or intentional destruction of computing equipment								
	2.00	2.40	2.20	2.29	2.50	4.00	2.11	2.56
Electronic theft, sabotage or intentional destruction / disclosure of proprietary data or information								
	1.60	1.20	2.10	1.86	2.50	2.00	2.22	1.33
Virus infections or disruptive software								
	2.20	2.20	2.40	2.71	2.50	3.00	2.00	1.33
Denial of service								
	3.20	1.40	2.50	1.71	2.50	2.00	2.44	2.56
System failure or data corruption								
	2.40	3.60	3.60	2.71	3.00	2.00	1.89	2.44

Table 6: Crosstab of users' responses on the financial impact caused by security incidents

	Role within the institution									
	Management (10)		**Educator (17)**		**IT Personnel (3)**		**Other (18)**		**Response Percent**	
Awareness	**High (5)**	**Medium (5)**	**High (10)**	**Medium (7)**	**High (2)**	**Medium (1)**	**High (9)**	**Medium (9)**	**High**	**Medium**
Nothing	3	1	2	1	0	0	1	2	23.1 %	18.2%
Less than £1,000	1	0	0	0	0	0	0	1	3.8%	4.5%
Between £1,000-£10,000	0	0	0	1	0	0	1	0	3.8%	4.5%
Between £10,001-£50,000	0	0	0	0	0	0	0	0	0.0%	0.0%
More than £50,000	0	1	0	0	0	0	0	0	0.0%	4.5%
Insignificant	0	0	1	0	0	1	1	0	7.7%	4.5%
Unknown	1	3	7	5	2	0	6	6	61.5 %	63.6%

Controls for providing information security can be physical, technical, or administrative, and can be further classified as either preventive or detective. Preventive controls attempt to avoid the occurrence of unwanted events, whereas detective controls attempt to identify unwanted events after they have occurred. Preventive controls inhibit the free use of computing resources and therefore can be applied only to the degree that users are willing to accept them. Yang et al. (Yang et al., 2002) suggested that institutions should be obliged to have effective mechanisms for security and privacy controls and management.

At present, information security technology hardware and software are being used to secure eLearning environments either as the preventive or detective control. Basically the controls are the physical and technical means, for example the usage of identification card to enter the building and the usage of firewall for servers. The security that can be achieved through physical and technical means is limited, and should be supported by appropriate management and procedures. Without proper management, these controls are insufficient. Information security management approaches shall be implemented to secure eLearning.

Information security management is regarded as an administrative control. It includes policies, processes, procedures, organisational structures and software and hardware functions. A security policy is a formal statement of principles to secure an organization; which will represent the process and procedures. Process describes the act of taking something through an established and usually routine set of procedures to achieve the policy. Organisation structures are a hierarchical concept of subordination of entities in eLearning that collaborate and contribute to serve one common aim; to secure eLearning. Software and hardware functions will explain on the use of the software and hardware. Kritzinger & Von Solms (2006) have outlined four main elements of information security within eLearning: governance; policy and procedures; countermeasures; and monitoring the countermeasures. These elements are the information security management aspects in order to ensure that security implementation achieves its objectives. Hence the elements can be further detailed by considering information security threats and the users' roles

Information security management requires participation by all users in the organisation. Based on the survey conducted, it can be concluded that user are not fully participate and aware with the security situation in eLearning. Therefore as part of information security management elements, effective security awareness programs need to be implemented. These programs can help to increase users' level of tolerance for preventive controls by helping them understand how such controls enable them to trust their computing systems.

The success of eLearning requires facing all the challenges inherent in implementing eLearning, especially the information security challenge. Security aspects such as the availability, integrity and confidentiality of material and information will contribute to building a secure and safe eLearning environment. This study has focus only on the supply group and should be expanded to the demand group. The future research can be conducted to identify the perception of the students towards the information security threats in the eLearning environment.

7. Conclusion

ELearning has grown and is continuing to grow very fast; the benefits it offers have increased the number of eLearning users substantially. The functionality of eLearning keeps on expanding, and relies heavily on the Internet. However the commission of illegal activities on the Internet has made it a place which exposes eLearning to threats. In order to ensure the availability and integrity of information and material in eLearning environments, countermeasures such as security technology hardware and software have been implemented. Nevertheless, these are considered insufficient. Information security management is needed to safeguard the security of an eLearning environment, and because of the flexibility factor offered by eLearning and the behaviour of different users, eLearning needs a security management framework that can guide eLearning providers (institutions) in managing information security in eLearning environments. Empirical data has indicated that different users have similar perceptions of eLearning security; hence users could share a similar framework. This combination of information security management and current information security technology could allow better results in terms of successful security implementation.

Acknowledgements

Special thanks to the Ministry of Higher Education (Malaysia) for sponsoring my research. I would also like to thank the experts in the eLearning team at Cranfield who helped me to validate the questionnaire. Last but not least, I thank the respondents who were willing to give their time and answer my questionnaire.

References

Adams, A. and Blandford, A. (2003), "Security and Online Learning: to Protect or Prohibit", in Ghaoui, C. (ed.) *Usability Evaluation of Online Learning Programs,* Information Science Publishing, London, pp. 331-359.

Allen, E. and Seaman, J. (2007), *Online Nation Five Years of Growth in Online Learning,* 1, Sloan Consortium, United States.

Alwi, N. H. M. and Fan, I. (2009), "Information Security Management in ELearning", *Internet Technology and Secured Transactions, 2009. ICITST 2009.International Conference for Internet Technology and Secured Transactions,* 9-12 November, London, IEEE Xplore, London UK, .

Chin, P. (2004), *Using C&IT to support teaching,* RoutledgeFalmer, London.

El-Khatib, K., Korba, L., Xu, Y. and and Yee, G. (2003), "Privacy and security in ELearning.", *International Journal of Distance Education Technologies,* vol. 1, no. 4, pp. 1-19.

Hamid, A. A. (2002), "eLearning Is it the “e” or the learning that matters?", *The Internet and Higher Education,* vol. 4, no. 3-4, pp. 311-316.

Jain, K. K. and Ngoh, L. B. (2003), "Motivating Factors in eLearning -a Case study of UNITAR", *Student Affairs Online,* [Online], vol. 4, no. 1, pp. 21 June 2008 available at: http://www.studentaffairs.com/ejournal/Winter_2003/eLearning.html.

Khan, B. H. (2004), "People, process and product continuum in eLearning: The eLearning P3 model", *Educational Technology,* vol. 44, no. 5, pp. 33-40.

Kritzinger, E. and von Solms, S. H. (2006), "ELearning: Incorporating Information Security Governance", *Issues in Informing Science and Information Technology,* vol. 3.

Lim, C. C. and Jin, J. S. (2006), "A Study on Applying Software Security to Information Systems: ELearning Portals", *IJCSNS,* vol. 6, no. 3B, pp. 162.

Norman, S. and Da Costa, M. (2003), "Overview of eLearning Specifications and Standards", *Open Learning Agency, and Eduspecs Technical Liaison Office,* .

Raitman, R., Ngo, L. and Augar, N. (2005), "Security in the Online ELearning Environment", *Advanced Learning Technologies, 2005.ICALT 2005.Fifth IEEE International Conference on Advanced Learning Technologies,* , pp. 702-706.

Yang, C., Lin, F. O. and Lin, H. (2002), "Policy-based Privacy and Security Management for Collaborative E-education Systems.", *Proceedings of the 5th IASTED International Multi-Conference Computers and Advanced Technology in Education (CATE 2002),* , pp. 501–505.